Contract No. NASw - 572 Westinghouse Reference WGD - 38531

RESEARCH ON FAILURE FREE SYSTEMS

Quarterly Report No. 8

Covering the period March 23, 1966 to June 23, 1966

Prepared for:

The National Aeronautics and Space Administration
Washington, D.C.

Westinghouse Defense and Space Center
Surface Division
P. O. Box 1897 Baltimore 3, Md.

Report Objectives and Contract Status Statement

This quarterly report is prepared in accordance with the requirements of contract NASw - 572, between the Westinghouse Electric Corporation and the National Aeronautics and Space Administration. The report describes the work which has been done during the second quarter of the contract extension established by modification No. 5 of this contract. The work to date represents completion of approximately 65% of the extension effort.

A. BROAD PROGRAM OBJECTIVE

The general objective of this research program is to consider new techniques which can be expected to offer significant increases in the reliability of vital electronic systems. These increases can normally be realized by giving the systems the capability to withstand a relatively large percentage of internal component failures without loss of system functional operation. The scope of this program has included the study of error detecting and error correcting codes, the problems associated with the operation and maintenance of redundant equipment, new schemes for permitting redundant system reorganization in response to changing failure patterns, adaptive logic networks and others.

B. SPECIFIC OBJECTIVES OF THE PRESENT PHASE OF THE PROGRAM

The present phase of the effort has been divided into two distinct sections. The first, smaller portion, provides for the documentation of a computer simulation program which was developed under a previous phase of this contract. The program itself provides a means for performing reliability analyses of a wide variety of failure responsive redundant systems. The objective of the major portion of this phase of the contract is the development of computerized procedures for efficiently allocating a limited number of test points within a redundant system and for estimating the system reliability when one or more components may have failed at the time of estimation.

C. STATUS OF THE COMPUTER PROGRAM DOCUMENTATION

Special Technical Report No. 6, documenting the Failure Responsive

Systems computer simulation program, was distributed in May. It is of interest to note that this simulation program is expected to be used extensively in performance of contract No. DA-28-AMC-023(E) concerning the investigation of self-repair techniques. This one year contract, between Westinghouse and U.S. Army Electronics Command, was initiated June 1, 1966.

D. TECHNICAL ACTIVITY AND STATUS OF THE TEST POINT ALLOCATION AND RELIABILITY ESTIMATION TASKS

The second quarterly report indicated that the block model reliability analysis procedure, developed by D. K. Rubin[1], of J.P.L., was being considered as an alternative to the minimal cuts reliability analysis procedure. That report described several advantages to be expected from such a change in analysis technique.

At this time, Mr. Rubin has shown that the block model is more accurate than the minimal cuts technique in estimating the reliability of series-connected triple modularly redundant majority-voted networks. Although it has not been proved that the block model reliability estimate is always more accurate for complex systems involving multiple fan-in, fan-out, feedback and feedforward, the comparison of reliability estimates for several specific systems indicates that the block model is more accurate than the minimal cuts model for most practical systems. In certain cases, where extremely long feed-back loops are present, it appears that the block-reliability analysis may give a more pessimistic reliability estimate than the minimal cuts analysis procedure.

1. "The Placement of Majority Voters within Modularly Redundant Digital Systems", by D. K. Rubin, Masters Thesis, University of California, Los Angeles.

After carefully comparing the various aspects of the minimal cuts analysis and the block reliability analysis, the decision was made in April 1966 to use the latter as the basis for the reliability estimation procedure being developed for the present program. The first step toward practical utilization of this analysis procedure was to write a general computer program which could provide an estimate of the reliability of almost any digital system given that all units in the system were known to be working at the time of the estimate.

Such a program has been written in FORTRAN IV. Several test problems have been run on the program, and the results support the hypothesis that the model does produce a lower bound which is greater than or equal the minimal cuts model for complex-connected systems. The program itself is significantly simpler in concept and requies much fewer instructions than the computer implementation of the minimal cuts model.

This program has provided the base for the final computer program required to estimate system reliability when all units are not known to be working at the time of test. Relaxing the assumption that all units must be working at the time the estimate is made, introduces a number of interesting problems. A few of these problems are described below.

Figure 1 shows one rank of a triplicated system with two test points[2], A and B. At the time of test, if test point A detects an error indicating

2. Important Note: Test points have been redefined to mean a source of information that indicates whether the signal at that point is in error. This is in contrast to the assumption that a test point would reveal the exact operational state of a particular unit (subsystem). This redefinition greatly complicates the analysis, but is much more practical in terms of the hardware implementation considerations.

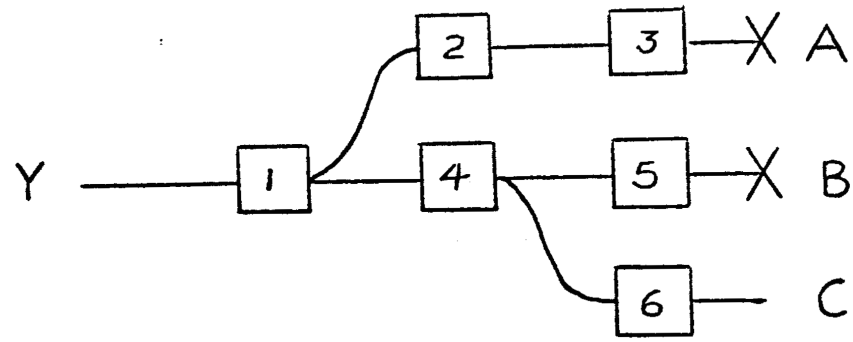

Figure 1 - One Rank of an Example System
with no Voters Between Y and A B or C.

a string failure in units 1, 2, or 3, and point B shows no failure, units 2 and 3 can be considered failed, and 1, 4, and 5 can be considered working. The probability that the string consisting of units 2 and 3 is working at test is 0, while the probability the units 1, 4 and 5 are working is 1. The probabilities that 1, 4, and 5 work until the mission is completed can be computed using the respective failure rates for the units together with the information that they were working at the time of testing. The probability that unit 6 is working at test time, and the probability that it will work until mission time are both computed from the failure rate information alone since there is no additional information from the test data.

A more complex situation could occur, in which a unit appears in one or more failed strings, and also appears in an untested string. In this case, the probability that the unit is working cannot be set to zero, since it must be used in the estimation of the untested string's reliability. The unit's reliability is calculated from the failure rates of all the units in the failed strings, with the condition that at least one of these units is failed.

During this quarter, techniques have been developed for including test information in the reliability estimation procedure. These techniques are now being implemented as additions to the block reliability analysis computer program. At the present time most of the programming changes have been made, but the new version of the program has not yet been punched onto cards and run. The completion of this program will mark the accomplishment of one of the major project goals - development of a practical technique for estimating system reliability based on partial system test.

It should be noted that in order to take advantage of the reference signals inherent in redundant systems, it is presently being assumed that all test points are comparator type circuits, which compare two of the replicated signals to disclose failures. This eliminates the need for the generation of an external reference signal during test. It is further being assumed that each tested location will have two such comparator test points, so that the operation of all three ranks will be tested.

The comparator type test point is particularly advantageous for this application because the assumption is being made that the system will be exercised sufficiently to confirm overall system operation at the time of test. When such an exercise is performed, the simple comparator type test point will detect failures in any unit except certain input failures in majority voters.

The second major goal of the project is to develop a practical technique for optimumally allocating a limited number of test points to the possible test point "sites" in a large redundant system. This phase of the project was expected to require the use of the reliability analysis procedure discussed above. The effort on this task has, therefore, been oriented toward the development of a suitable value (or objective) function which could be optimized to provide a correlated optimum pattern of test point locations. The success of this effort has been frustrated by a number of problems all of which are related to the single problem of defining what the actual value of any test is.

The necessity of having a suitable value function before further work on this task can be fruitfully continued has resulted in a reduction in the level of effort by all contract personnel except the project engineer. The development of a value function by the project engineer will be followed by an immediate resumption in level of effort by other project personnel to complete the necessary programming and documentation. In order to fully meet the project objectives a two month, no-cost, extension has been requested and granted.

E. TECHNICAL ACTIVITIES PLANNED FOR THE REMAINDER OF THE CONTRACT

1. Development of a Generalized Value Function
2. Programming of the allocation procedure
3. Completion and test of the Modified Block Reliability Analysis Computer Program
4. Test of the allocation procedure by allocation of a limited number of test points to the J.P.L. Redundant Spacecraft Sequencer
5. Document the allocation procedure and the analysis procedure computer program in detail
6. Prepare a final report

G. MANAGEMENT AND PERSONNEL

The management of this contract continues to be performed by the Advanced Development Subdivision of the Surface Division of the Westinghouse Defense and Space Center. The management personnel with primary responsibility for this program include:

Mr. Sydney E. Lomax, Director of Development

Mr. Theodore Hamburger, Supervisory Engineer

The technical personnel assigned to the program during this contract quarter include:

Mr. Charles G. Masters, Jr., Project Engineer

Mr. Frank B. Cole, Sensior Engineer

Mr. Joseph M. Hannigan, Associate Engineer